REMARKS

The Examiner rejected portions of the disclosure and the title. This amendment corrects those areas.

The new claims presented herein include more detail to distinguish the cited references. These new claims add no new matter.

The Examiners rejected claims 1, 3, 5, 11 and 13 under 35 112, second paragraph, citing indefiniteness. The new claims have been reviewed to ensure that these types of errors are not present.

The Examiner rejected claims 1, 3 and 13 under 35 USC 102(e) citing U.S. pat. no. 6,108,420 to Larose et al. (Larose). The remaining claims were rejected under 35 USC 103(a) using Larose as the primary reference and U.S. patents no. 6,240,513 to Friedman et al. (Friedman) and then U.S. pat. no 6,026,166 to LeBourgeois (LeBourgeois).

A new set of claims is presented in this amendment, but the Examiner's finding in the office action are instructive. On page 5, paragraph 13, the Examiner determined that "Larose is silent on the matter of encrypting the software product using the first value..." Later in the same paragraph the Examiner determined that "using keys that are derived from device/system parameters are commonly implemented in the art." The Examiner used Larose as anticipating the claims that did not have the computer parameters cited as a source of a key, and Larose and Friedman as suggesting the claims that had the computer parameters, and Larose, Friedman and Lebourgeois as suggesting the claims con-

taining a "quorum." As a general comment (more detail follows) these prior art references all require the use of PPK's (Public/Private Keys). Larose states this requirement directly, Friedman also generates PPK's and LeBourgeous's signatures are based on PPK's, and the only reasonable way of combining them includes use of these PPK's. As such all of these prior art patents require the transfer or sendingof at least a public key, and such a transfer is a weakness acknowledged (see below) in Larose, that is not found in the present claims as now amended.

The following will discuss the new claims with respect to Larose, Friedman and LeBourgeois in more detail with respect to the present claims.

New claim 16 includes these limitations:

> *encrypting, at the server computer, the software product using the single value as an encryption key,*
>
> .....
>
> *decrypting the encrypted software application by using the single value as the decryption key.*

Also in claim 16, the single value itself is encrypted and decrypted using the identical members of a set of parameters, as follows:

encrypting, at the server computer, the single value by using members of the first set of parameters as encryption keys, and...

decrypting members of the set of encrypted single values using members of the second set of parameters as decryption keys

Please note that the present invention, as now claimed, uses the single value to encrypt and to decrypt the software application. This defines a symmetric encryption key as contrasted to the PPK (private/public key). New claim 16 also contains another sym-

metric encryption key using the parameters to encrypt and to decrypt. In contrast, Larose describes a system that requires the use of PPK at col. 7, lines 12-29:

> *i)...the production of a cryptographic fingerprint..., and*
> *ii)protection of that cryptographic fingerprint by encrypting it with a private key that the recipient of the fingerprint may, by using a public key and cryptographic algorithm, verify that the data is intact....These two steps are essential to realize that advantages of the present invention, since without both steps a third party may intervene and alter data without the recipient being able to detect it.*

These "private" and "public" keys are created by using "Public-Private Key (PPK) encryption algorithms" as discussed throughout Larose (e.g., see Larose Column 7 lines 41; Column 7 lines 34 – Column 8 lines 27, Fig. 2, "public/Private key pairs" 150, and in Figs. 3a, 3b, and 3c: the "PPK encryption algorithms" 113, "public key" 152, and the "private key" 151). Therefore, the elements in the claims of the present invention, which disclose processes for using symmetric keys, that are created from information collected from the installation computer, are not found or suggested in Larose.

The excerpt above from Larose requires the use of PPK's, where a public key must be transferred unencrypted to a user to verify a digital signature. Larose acknowledges that the unencrypted public key is a security risk, see Larose col. 13, lines 59-64. The present invention advantageously uses symmetric keys. Moreover, with respect to transferring keys as is necessary in the cited prior art, the parameters from which the keys are developed, but not the keys themselves, are only transferred in the present claims.

Furthermore, Larose is silent on elements of claims 26, 28, and 30: of generating a second set of parameters and comparing this second set with a first set before the software product is downloaded, and then authorizing the starting of a download, and does not disclose the following element of claims 21 and 33: *requesting access to the encrypted software product at the computer, and in response thereto, generating a second set of data from the computer,* among other elements in these claims.

Similarly, Larose is silent on elements of claim 33:

moving said software product to a second computer,
requesting access to the software product, and in response thereto,
generating a first set of parameters from the second computer, and
not authorizing the execution of the software product on the second computer.

Larose, combined with Friedman, does not anticipate or suggest the new claims.

Since Larose requires and only discloses the use of PPK's, any other secondary reference that may be joined to Larose must retain that PPK use, or, the secondary reference will be contrary to Larose's teachings. With this in mind and that the present claims are limited to symmetric keys f Larose is distinguished. Larose should be completely removed as a reference.

It then follows that Friedman and/or Lebourgeois cannot be combined with Larose to suggest the present invention as now claimed.

Friedman, as primary reference, does not anticipate or suggest the new claims.

Considering Friedman as the primary reference does not help.

Friedman is also reliant upon the use of PPK's. The first 2 keys created, from a total of 6, are static and dynamic private keys, both generated when Friedman's security device is turned on. (Friedman Column 10 lines 21-22 and see Fig. 4a item 400). The static private key, which is not a symmetric key, is created from a "seed" from the security device (as opposed to the client host, see Column 10 lines 27-33 and Fig. 4a item 400 vs. item 404). The dynamic private key is then randomly generated and derived from seeds obtained from seconds, minutes, etc. The static and dynamic public keys are then generated from these private keys from the equation on Column 10 line 63. When the "client host" *first* sends a message to another network security device: "*a protocol is executed by which the two devices (i) exchange static public keys (unencrypted).*"

This required usage of PPK, and the subsequent exchange of public keys between the security devices, is the enabling basis for all subsequent operations necessary for the operation of the Friedman invention (see Friedman Column 11 lines 5-6, also Fig. 8 steps 836, and Column 9 lines 26-28) and is in contrast with the present invention—which is not reliant upon PPK, and an exchange of public keys, to create and utilize symmetric keys.

Also, Friedman does not generate parameters from the installation computer nor does he send such collected information to a sever computer, nor does he create a symmetric key from this information, is silent on encrypting/decrypting software products, on "streaming data," and on *authorizing access to the software product at the user's computer, requesting access to the encrypted software product at the computer, and in response thereto, generating a second set of data from the computer, authorizing the execution of the software product on the computer.* Therefore, Friedman does not disclose the relevant claim elements of claims 16-20 and claim 23.

In addition, Friedman is silent on elements of claims 21: generating a second set of parameters and comparing this second set with a first set before the software product is downloaded, and then authorizing the starting of a download.

Similarly, Friedman is silent on elements of claim 24: *moving said software product to a second computer, and requesting access to the software product, and in response thereto, generating a first set of parameters from the second computer, and not authorizing the execution of the software product on the second computer.*

Therefore it is respectfully requested that a notice of allowance be issued for the present invention as now claimed.

PATENTS
159008-0003

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

Edwin H. Paul
Reg. No. 31,405
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500